first multiplier signal to a first multiplier input line,

B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,

C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a second multiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and

D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary **1**, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

35. In the communications system according to claim **33** where e is relatively prime to the Euler totient function of n, $\emptyset(n)$, and where $a_e=1$ and $a_{e-1}, \ldots, a_0$ equal zero,

a decoding means adapted for receiving C and for transforming C to a receive message word signal M',

where M' corresponds to a number representative of a deciphered form of C and corresponds to

$$M' \equiv C^d \pmod{n}$$

where d is a multiplicative inverse of e(mod(λ(n))) where $\lambda(n)$ is the least positive integer such that

$$S^{\lambda(n)} \equiv 1 \pmod{n}$$

for all integers S relatively prime to n.

36. In the communications system according to claim **33** where said encoding means is adapted to transform M to C by the performance of a first ordered succession of invertible operations on M, at least one of said operations being exponentiation, a decoding means adapted to transform C to M by the performance of a second ordered succession of invertible operations on C, wherein each of the invertible operations of said second succession is the inverse of a corresponding one of said first succession, and wherein the order of said operations in said second succession is reversed with respect to the order of corresponding operations in said first succession.

37. A method for establishing cryptographic communications comprising the step of:

encoding a digital message word signal M to a ciphertext word signal C, where M corresponds to a number representative of a message and

$$0 \leq M \leq n-1$$

where n is a composite number and

where C corresponds to a number representative of an encoded form of message word M,

wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$$

where e and $a_e, a_{e-1}, \ldots a_0$ are numbers.

38. In the method according to claim **37** where e is relatively prime to the Euler totient function of n, $\emptyset$n), and where $a_e=1$ and $a_{e-1}, \ldots, a_0$ equal zero, the further step of:

decoding said ciphertext word signal C to said message word signal M,

wherein said decoding step comprises the step of:

transforming said ciphertext word signal C, whereby:

$$M \equiv C^d \pmod{n}$$

where d is a multiplicative inverse of e(mod(λ(n)) where $\lambda(n)$ is the least positive integer such that

$$S^{\lambda(n)} \equiv 1 \pmod{n}$$

for all integers S relatively prime to n.

39. In the method according to claim **37** where said encoding step includes the step of transforming M to C by the performance of a first ordered succession of invertible operations on M, the further step of:

decoding C to M by the performance of a second ordered succession of invertible operations on C, where each of the invertible operations of said second succession is the inverse of a corresponding one of said first succession, and wherein the order of said operations in said second succession is reversed with respect to the order of corresponding operations in said first succession.

40. A method according to claims **23** or **24** or **25** or **26** or **27** or **28** or **29** or **30** or **31** or **32** or **37** or **38** or **39** wherein at least one of said transforming means comprises the steps of:

receiving and storing a first digital signal in a first register, said first digital signal being representative of said word-to-be-transformed,

receiving and storing a second digital signal in a second register, said second digital signal being representative of the exponent of the equivalence relation defining said transformation,

receiving and storing a third digital signal in a third register, said third digital signal being representative of the modulus of the equivalency relation defining said transformation, and

exponentiating said first digital signal by repeated squaring and multiplication using said second and third digital signals, said exponentiating step including the substeps of:

A. receiving and storing a first multiplier signal in an output register, and applying said first multiplier signal to a first multiplier input line,

B. successively selecting each of the bits of said second digital signal as a multiplier selector, and

C. for each of said multiplier selectors, selecting as a second multiplier signal either the contents of said output register or the contents of said first register, and for applying said second multiplier signal to a second multiplier output line, said selection being dependent on the binary value of the successive bits of said second digital signal,

D. for each of said multiplier selectors, generating said first multiplier signal in a modulo multiplier